REMARKS/ARGUMENTS

This Response to Office Action is filed within six months of the mailing date of the Office Action from the Examiner mailed February 16, 2006. Reconsideration and withdrawal of the rejections set forth in the Office Action is respectfully requested. Claims 1-3, 10-12, 19, 25 and 31-44 are pending in this application.

THE PRIOR ART (Vahalia et al.)

Vahalia et al. apparently disclose a network file server sharing local caches of file access information in data processors assigned to respective file systems. The Examiner indicates at page 3 of the Office Action:

> The system processes and receives NFS data requests from a client computer (Col. 13, lines 66-67), which meets the limitation of providing a network file system on a client, wherein said network file system handles and forwards requests from streaming-enabled local processes on said client that are directed at streaming application programs files located on said server. The data is provided over the system in a streaming fashion (Col. 7, lines 13-29).

The applicants respectfully disagree. Vahalia et al. do not describe streaming-enabled local processes. Streaming media has been used for some time, and streaming software was invented more recently. In both cases, a local process that is streaming-enabled means that the local process is capable of receiving a data stream and playing or running an associated file or program before all of the data has been received. Although all computers are capable of receiving a data stream, which is a different use of the term "stream" than used for streaming media or streaming software, not all computers are necessarily streaming-enabled due to this difference in meaning. Vahalia et al. do not describe streaming media or streaming software and, accordingly, do not suggest or imply a NFS that "handles and forwards requests from streaming-enabled local processes" or requests "that are directed at streaming application program files."

This observation is supported by the text cited by the Examiner at col. 7, lines 13-29, where Vahalia et al. describe streaming data for archival. Indeed, Vahalia et al. use the word streaming as follows:

> ...the cached disk storage subsystem 23 can absorb a
> high data inflow aggregation from tens or hundreds of
> network links streaming from multiple sites, and balance
> this load on the read/write stations 41.

As is apparent from this text, Vahalia et al. refer to streaming from multiple sites as, quite simply, sending a data stream, rather than in the more sophisticated multimedia or software streaming contexts in which one would use the terms "streaming-enabled" or "streaming application program files."

Applicable to Claims 32, 33, 35, 36, 38-41, 43, 44

The Examiner indicates at page 8 of the Office Action:

> Clients have a security level associated with them in
> order to control access to files containing sensitive
> material (Col. 17, lines 7-10), which meets the limitation
> of determining whether the section of said streaming
> application program files that is being requested is a
> critical section.

The applicants respectfully point out that recognizing sensitive information is not the same as identifying a critical section that requires protection from piracy. For example, a streaming server may have customer personal information that is sensitive and may be read-locked, but the streaming server may also include a streaming file that would be desirable to a potential pirate. The protection associated with the sensitive customer information and the streaming file is different. For example, all streaming clients may have access to the streaming file, but the streaming file may still include a critical section. If the streaming clients (even one) were blocked access to the streaming file, then the streaming clients may not be able to execute the streaming program at all (or at least that section of it).

Moreover, Vahalia et al., at col. 17, lines 7-10, describe a standard document management system lock. For example, if a word processing document is opened for read/write access by one client, another client cannot open the file to perform writes. This is so that the document does not have two competing versions open at the same time. Vahalia et al. explain that one client may be able to override the lock of another client. Streaming files on the server, on the other hand, are normally not modified by clients. So, all of the streaming files could be characterized as "write-locked" with respect to the streaming clients. Vahalia et al. do not describe a system that would even work in a streaming context.

The Examiner indicates at page 8 of the Office Action:

> Applicant's specification (page 4) defines a pattern of
> piracy as an attempt to copy as opposed to code
> execution. Vahalia discloses that each file contains read
> and write locks that can be enabled depending on how
> the content owners want the content to be accessed.
> The locks can be enabled so that the content can only be
> read or code executed, and if the client requests to write
> the file, then the request is denied (Col. 17, line 58 – Col.
> 18, line 8), which meets the limitation of determining
> whether an originating process making the request for
> access exhibits a pre-determined pattern of piracy.

The applicants respectfully disagree with the Examiner's characterization of the prior art. Applicant's specification (page 4) defines an example of a pattern of piracy as an attempt to copy the data as opposed to page in the data as code for execution. The reason why this potentially allows one to surmise the purpose of the request is that in a streaming software context, a streaming application is executed before all streaming files have been received. The streaming files are typically requested on the fly, as the need arises. If a request was made to copy files, instead of receive the files in a manner that is consistent with the execution of the streaming application, that may enable one to surmise that the access is by a potential pirate.

The Examiner's implication appears to be that the use of read/write locks by Vahalia et al. is equivalent to determining whether an originating process making the request for access exhibits a pre-determined pattern of piracy. The applicants respectfully assert that the system described by Vahalia et al. would not enable a person of ordinary skill in the art to determine that an originating process exhibits a pre-determined pattern of piracy. No hint may be gleaned from the locking of the files, and Vahalia et al. provide not even the most tenuous hint of such a teaching. Indeed, the Examiner must read from the applicant's disclosure to find a hint regarding how a pre-determined pattern of piracy might be identified, since none is found in the prior art. Therefore, the applicants respectfully request that the Examiner withdraw this assertion.

THE PRIOR ART DISTINGUISHED (Vahalia et al.)

The Examiner rejected claims 1-3, 10-12, 19, 25 and 31-44 under 35 U.S.C. 102(e) as allegedly anticipated by U.S. Pat. No. 6,192,408 (Vahalia et al.).

Independent Claim 1

Claim 1 includes, in part, the language "said network filesystem handles and forwards requests from steaming-enabled local processes on said client that are directed at streaming application program files located on said server".

To anticipate a claim, a reference must teach each and every limitation of the claim.

Since Vahalia et al. do not teach streaming-enabled processes, or in the alternative Vahalia et al. do not teach streaming application program files, Vahalia et al. do not anticipate claim 1. Claims 2 and 3, which depend from claim 1, are allowable at least for depending from an allowable base claim.

Independent Claim 10

Claim 10 includes, in part, the language "said network filesystem handles and forwards all requests from steaming-enabled local processes on said client that are directed at streaming application program files located on said server".

Since Vahalia et al. do not teach streaming-enabled processes, or in the alternative Vahalia et al. do not teach streaming application program files, Vahalia et al. do not anticipate claim 10. Claims 11 and 12, which depend from claim 10, are allowable at least for depending from an allowable base claim.

Independent Claim 19

Claim 19 includes, in part, the language "said filesystem handles and forwards file requests from streaming enabled local processes on said client". Since Vahalia et al. do not teach streaming-enabled processes, Vahalia et al. do not anticipate claim 19.

Independent Claim 25

Claim 25 includes, in part, the language "said filesystem handles and forwards all file requests from streaming enabled local processes on said client". Since Vahalia et al. do not teach streaming-enabled processes, Vahalia et al. do not anticipate claim 25.

Independent Claim 31

Claim 31 includes, in part, the language "using a first computer to serve streaming application program files to a second computer for streaming execution". Since Vahalia et al. do not teach streaming application program files, Vahalia et al. do not disclose any streaming execution and, therefore, do not anticipate claim 31.

Independent Claim 32

Claim 32 includes, in part, the language "providing information relating to one or more remote locations where streaming application program files are stored". Since Vahalia et al. do not teach streaming application program files, Vahalia et al. do not anticipate claim 32.

In addition, Claim 32 includes, in part, the language "whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said streaming application program files that is being requested is a critical section that requires protection from piracy." Since Vahalia et al. do not teach piracy protection techniques as described in claim 32, Vahalia et al. do not anticipate claim 32 for this additional reason.

Independent Claim 33

Claim 33 includes, in part, the language "if it is determined that a history of previous requests for access made by said originating process lacks a pre-determined pattern of piracy or that a section of said streaming application program files that is being requested is a non-critical section, then forwarding said request to a corresponding remote server that is responsible for serving said streaming application program files." Since Vahalia et al. do not teach streaming application program files, Vahalia et al. do not anticipate claim 33. Since Vahalia et al. do not teach piracy protection techniques as described in claim 33, Vahalia et al. do not anticipate claim 33 for this additional reason.

Independent Claim 34

Claim 34 includes, in part, the language "using a filtering mechanism on a client computer for filtering requests for access to streaming application program files". Since Vahalia et al. do not teach streaming software application program files, Vahalia et al. do not anticipate claim 34.

Independent Claim 35

Claim 35 includes, in part, the language, "whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said streaming application program files that is being requested is a critical section that requires protection from piracy." Since Vahalia et al. do not teach streaming application program files, Vahalia et al. do not anticipate claim 35. Since Vahalia et al. do not teach piracy protection techniques as described in claim 35, Vahalia et al. do not anticipate claim 35 for this additional reason.

Independent Claim 36

Claim 36 includes, in part, the language, "whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said streaming application program files that is being requested is a critical section that requires protection from piracy." Since Vahalia et al. do not teach streaming application program files, Vahalia et al. do not anticipate claim 36. Since Vahalia et al. do not teach piracy protection techniques as described in claim 36, Vahalia et al. do not anticipate claim 36 for this additional reason.

Independent Claim 37

Claim 37 includes, in part, the language, "a filtering means for filtering requests for access to streaming software application program files stored remotely from said filtering means." Since Vahalia et al. do not teach streaming software application program files, Vahalia et al. do not anticipate claim 37.

Independent Claim 38

Claim 38 includes, in part, the language, "determining whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said streaming application program files that is being requested is a critical section that requires protection from piracy." Since Vahalia et al. do not teach streaming application program files, Vahalia et al. do not anticipate claim 38. Since Vahalia et al. do not teach piracy protection techniques as described in claim 38, Vahalia et al. do not anticipate claim 38 for this additional reason.

Independent Claim 39

Claim 39 includes, in part, the language, "after examining said request and if it is determined that an originating process that is making said request for access is a trusted process, and that a history of previous requests for access made by said originating process lacks a pre-determined pattern of piracy, and that a section of said application program files that is being requested is a non-critical section, then forwarding said request to a corresponding remote server that is responsible for serving said streaming application program files." Since Vahalia et al. do not teach streaming application program files, Vahalia et al. do not anticipate claim 39. Since Vahalia et al. do not teach piracy protection techniques as described in claim 39, Vahalia et al. do not anticipate claim 39 for this additional reason.

Independent Claim 40

Claim 40 includes, in part, the language, "determining whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said streaming application program files that is being requested is a critical section that requires protection from piracy." Since Vahalia et al. do not teach streaming application program files, Vahalia et al. do not anticipate claim 40. Since Vahalia et al. do not teach piracy protection techniques as described in claim 40, Vahalia et al. do not anticipate claim 40 for this additional reason.

Independent Claim 41

Claim 41 includes, in part, the language, "whether said requests can be granted based on whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said streaming application program files that is being requested is a critical section that requires protection from piracy". Since Vahalia et al. do not teach streaming application program files, Vahalia et al. do not anticipate claim 41. Since Vahalia et al. do not teach piracy protection techniques as described in claim 41, Vahalia et al. do not anticipate claim 41 for this additional reason.

Independent Claim 42

Claim 42 includes, in part, the language, "if said computer process is a trusted process, then forwarding said request to a corresponding remote server that is responsible for serving said streaming software application program files." Since Vahalia et al. do not teach streaming software application program files, Vahalia et al. do not anticipate claim 42.

Independent Claim 43

Claim 43 includes, in part, the language, "if history of previous requests of said computer process lacks a pre-determined pattern of piracy, then forwarding said request to a corresponding remote server that is responsible for serving said streaming application program files." Since Vahalia et al. do not teach streaming application program files, Vahalia et al. do not anticipate claim 43. Since Vahalia et al. do not teach piracy protection techniques as described in claim 43, Vahalia et al. do not anticipate claim 43 for this additional reason.

Independent Claim 44

Claim 44 includes, in part, the language, "if said section is a non-critical section, then forwarding said request to a corresponding remote server that is responsible for serving said streaming software application program files." Since Vahalia et al. do not teach streaming software application program files, Vahalia et al. do not anticipate claim 44.

THE PRIOR ART (Safadi et al.)

Safadi et al. apparently disclose a method and system for impulse purchasing of services over a communication network. Such services include streaming media. The access controller generates entitlements and a secure processor generates entitlement tokens by which security is provided. A token is generated for the service selected or purchased by the subscriber. The token is secure and signed.

Notably, Safadi et al. do not disclose software streaming. Streaming media is a well-known technique that enables a media stream to be run as it is received. Streaming software, however, is a much more recent invention that allows a program to be executed before it is installed. Streaming application files are provided as streaming software is executed.

<u>Applicable to Claims 32, 33, 35, 36, 38-41, 43, 44</u>

The Examiner indicates at page 24 of the Office Action:

> Safadi discloses a system for multimedia services
> wherein a user requests use of a specific data services
> by creating a secure entitlement token that can be
> authenticated by a client application at the subscriber
> terminal based on a credit amount (Col. 1, line 62 – Col.
> 2, line 10, Col. 3, lines 11-17), which meets the limitation
> of providing information relating to one or more remote
> locations where said application program files are stored,
> determining whether an originating process that is
> making said requests for access is a trusted process,
> whether a history of previous requests for access made
> by said originating process exhibits a pre-determined
> pattern of piracy, and whether a section of said
> application program files that is being requested is a
> critical section that requires protection from piracy.

Safadi et al., at Col. 1, line 62 – Col. 2, line 10, describe a subscriber credit validation technique and, at Col. 3, lines 11-17, describe a pre-authorized credit amount. After a careful reading of the Safadi reference, the applicant finds no suggestion, either explicit or implicit, to determine whether a history of previous requests for access made by an originating process exhibits a pre-determined pattern of piracy. Safadi et al. do not mention the word piracy or provide any mechanism or suggestion about how to identify a pre-determined pattern of piracy. Therefore, the applicants respectfully request that the Examiner withdraw this assertion.

Moreover, the applicants respectfully disagree that Safadi et al. disclose determining whether a section of the application program files that is being requested is a critical section that requires protection from piracy. The Examiner simply cites a portion of the Safadi et al. reference that describes a subscriber obtaining credit to access services. After a careful review of the Safadi et al. reference, the applicants can find no suggestion that a critical section of anything associated with the services is

determined, nor that a critical section that requires protection from piracy is identified or identifiable.

THE PRIOR ART DISTINGUISHED (Safadi et al.)

The Examiner rejected claims 31-44 under 35 U.S.C. 102(e) as allegedly anticipated by U.S. Pat. No. 6,810,525 (Safadi et al.).

Independent Claim 31

Claim 31 includes, in part, the language "using a first computer to serve streaming application program files to a second computer for streaming execution". Since Safadi et al. do not teach streaming application program files, Safadi et al. do not disclose any streaming execution and, therefore, do not anticipate claim 31.

Independent Claim 32

Claim 32 includes, in part, the language "whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said streaming application program files that is being requested is a critical section that requires protection from piracy." Since Safadi et al. do not teach piracy protection techniques as described in claim 32, Safadi et al. do not anticipate claim 32.

Independent Claim 33

Claim 33 includes, in part, the language "if it is determined that a history of previous requests for access made by said originating process lacks a pre-determined pattern of piracy or that a section of said streaming application program files that is being requested is a non-critical section, then forwarding said request to a corresponding remote server that is responsible for serving said streaming application program files." Since Safadi et al. do not teach piracy protection

techniques as described in claim 33, Safadi et al. do not anticipate claim 33 for this additional reason.

Independent Claim 34

Claim 34 includes, in part, the language "using a filtering mechanism on a client computer for filtering requests for access to streaming software application program files". Since Safadi et al. do not teach streaming software application program files, Safadi et al. do not anticipate claim 34.

Independent Claim 35

Claim 35 includes, in part, the language, "whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said streaming application program files that is being requested is a critical section that requires protection from piracy." Since Safadi et al. do not teach piracy protection techniques as described in claim 35, Safadi et al. do not anticipate claim 35.

Independent Claim 36

Claim 36 includes, in part, the language, "whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said streaming application program files that is being requested is a critical section that requires protection from piracy." Since Safadi et al. do not teach piracy protection techniques as described in claim 36, Safadi et al. do not anticipate claim 36.

Independent Claim 37

Claim 37 includes, in part, the language, "a filtering means for filtering requests for access to streaming software application program files stored remotely from said filtering means." Since Safadi et al. do not teach streaming software application program files, Safadi et al. do not anticipate claim 37.

Independent Claim 38

Claim 38 includes, in part, the language, "determining whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said streaming application program files that is being requested is a critical section that requires protection from piracy." Since Safadi et al. do not teach piracy protection techniques as described in claim 38, Safadi et al. do not anticipate claim 38.

Independent Claim 39

Claim 39 includes, in part, the language, "after examining said request and if it is determined that an originating process that is making said request for access is a trusted process, and that a history of previous requests for access made by said originating process lacks a pre-determined pattern of piracy, and that a section of said application program files that is being requested is a non-critical section, then forwarding said request to a corresponding remote server that is responsible for serving said streaming application program files." Since Safadi et al. do not teach piracy protection techniques as described in claim 39, Safadi et al. do not anticipate claim 39.

Independent Claim 40

Claim 40 includes, in part, the language, "determining whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said streaming application program files that is being requested is a critical section that requires protection from piracy." Since Safadi et al. do not teach piracy protection techniques as described in claim 40, Safadi et al. do not anticipate claim 40.

Independent Claim 41

Claim 41 includes, in part, the language, "whether said requests can be granted based on whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said streaming application program files that is being requested is a critical section that requires protection from piracy". Since Safadi et al. do not teach piracy protection techniques as described in claim 41, Safadi et al. do not anticipate claim 41.

Independent Claim 42

Claim 42 includes, in part, the language, "if said computer process is a trusted process, then forwarding said request to a corresponding remote server that is responsible for serving said streaming software application program files." Since Safadi et al. do not teach streaming software application program files, Safadi et al. do not anticipate claim 42.

Independent Claim 43

Claim 43 includes, in part, the language, "if history of previous requests of said computer process lacks a pre-determined pattern of piracy, then forwarding said request to a corresponding remote server that is responsible for serving said streaming application program files." Since Safadi et al. do not teach piracy protection techniques as described in claim 43, Safadi et al. do not anticipate claim 43.

Independent Claim 44

Claim 44 includes, in part, the language, "if said section is a non-critical section, then forwarding said request to a corresponding remote server that is responsible for serving said streaming software application program files." Since Safadi et al. do not teach streaming software application program files, Safadi et al. do not anticipate claim 44.

The applicants respectfully request the Examiner withdraw the rejections of claims 1-3, 10-12, 19, 25, and 31-44.

CONCLUSION

In view of the foregoing, Applicants submit that all the claims pending in the application patentably define over the prior art. The Applicants respectfully requests the Examiner withdraw rejections of all claims. A Notice of Allowance is therefore respectfully requested.

If extra fees are due, please charge our Deposit Account No. 50-0665 from which the undersigned is authorized to draw.

If in the opinion of the Examiner, a telephone conference would expedite the prosecution of the subject application, the Examiner is encouraged to call the undersigned at (650) 838-4305.

Respectfully Submitted,
PERKINS COIE LLP

Date: <u>May 16, 2006</u>

William F. Ahmann
Reg. No. 52,548

<u>Correspondence Address</u>:
Customer No. 22918
Perkins Coie LLP
P.O. Box 2168
Menlo Park, CA 94026
650-838-4300